OWNING THE WEATHER FOR INFORMATION OPERATIONS

Richard J. Szymber
Army Research Laboratory
Fort Huachuca, AZ 85635

Leander Page III
Office of the Deputy Chief of Staff for Intelligence
Washington, DC 20310

ABSTRACT

Situational awareness and the relevant common picture enable commanders to perceive changes in the environment and then act upon those changes to produce a desirable end state. Battlefield visualization of weather, and its effects, is an essential element of battle command, and is necessary for out-thinking the enemy and gaining information dominance. Owning the Weather (OTW) is the use of advance knowledge of the environment, and its effects on friendly and enemy personnel, systems, operations and tactics, to gain a decisive advantage over opponents. OTW technology and information systems (INFOSYS) can serve as a force multiplier by providing commanders and their staffs with known and predicted conditions and effects, enabling them to choose the time, manner, and place of engagement. OTW involves a four step process for knowing, applying, and integrating the weather: 1) battlespace sensing and data collection; 2) processing, forecasting, analysis, and dissemination; 3) battlefield visualization and decision aids; and 4) combat weather exploitation and information operations (IO). The objective of OTW IO is to guarantee and maximize our ability to exploit the weather to our advantage while simultaneously denying the enemy the ability to use or manipulate the weather to their advantage. This is accomplished by protecting our weather INFOSYS and attacking the enemy's INFOSYS, through weather C2W-protect and C2W-deny/influence operations, respectively. By the command and control warfare (C2W) methodology of data denial, we can limit threat force ability to know and forecast the weather conditions in the joint task force area of operations, thereby increasing our ability to win the information war and out-maneuver and out-fight the enemy. It is crucial to deny the enemy access to meteorological satellite information in order to maximize our advantage. Additionally, the enemy can be put at a disadvantage at a critical time and place if we could covertly modify their picture of the weather, thereby influencing them to take detrimental courses of action. And, possibilities exist for intercepting enemy weather data bases and transmissions without their knowing. OTW provides the capability to anticipate the differential impacts of weather on friendly and threat capabilities allowing commanders to exploit windows of opportunity created by the weather. Improved weather information and IO, combined with knowledge of the limitations of weather on warfighting capabilities, is a powerful information warfare weapon.

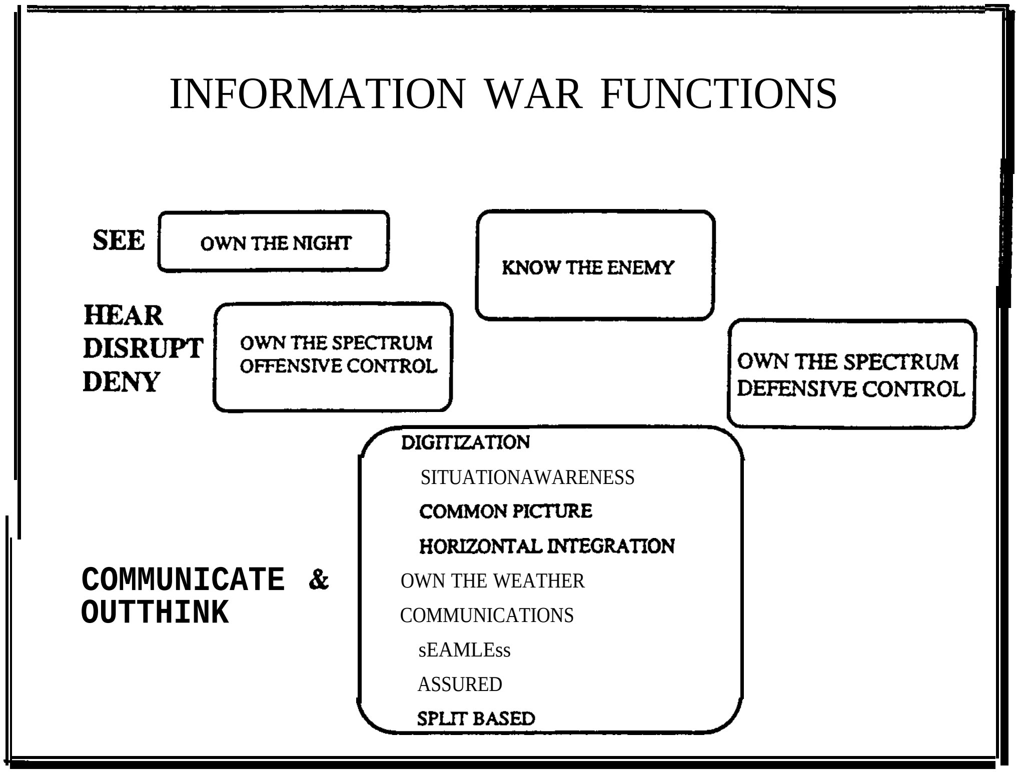
1.0 INTRODUCTION

Situational awareness and the relevant common picture give commanders the opportunity to understand adverse weather conditions exist or are forecast on a battlescale. In the era of Information Operations (IO), commanders can act on this advanced knowledge of environmental conditions and to use this knowledge for tactical advantage over threat forces. Battlefield visualization of weather, and its effects, is an essential element of battle command, and is necessary for out-thinking the enemy and gaining information dominance. Owning the Weather (OTW) is the use of advance knowledge of the environment, and its effects on friendly and enemy personnel, systems, operations and tactics, to gain a decisive advantage over opponents. OTW technology and information systems(INFOSYS) can serve as a force multiplier by providing commanders and their staffs with known and predicted conditions and effects, enabling them to choose the time, manner, and place to fight. The OTW vision describes a four step process for integrating weather into IO: 1) battlespace sensing and data collection; 2) processing, forecasting, analysis, and dissemination; 3) battlefield visualization and decision aids; and 4) combat weather exploitation through application to IO. OTW provides the capability to anticipate the differential impacts of weather on friendly and threat capabilities allowing commanders to integrate weather information into the decision process at targeting cells and therefore plan and exploit windows of opportunity created by adverse weather.

The objective of OTW IO has three parts. First, to guarantee commanders have high technology capabilities to receive and use surface and space based weather observations, battlescale weather forecasts, and weather effects on tactical operations. Second, to provide the comparative means to know when friendly forces will have advantage in adverse weather conditions before battles are fought . Third, to deny the threat forces the basic space based, high resolution information and high resolution forecast technology so they must fight without advance knowledge of the effects of adverse weather on their systems and personnel. This objective is accomplished by protecting our weather INFOSYS and attacking the enemy's INFOSYS, through weather C2W-protect and C2W-deny/influence operations, respectively. By the command and control warfare (C2W) methodology of data denial, we can limit threat force ability to know observed and forecast weather conditions in the joint task force area of operations, thereby increasing our ability to win the information war and out-maneuver and out-fight the enemy. It is crucial to deny the enemy access to meteorological satellite information in order to maximize our advantage. Additionally, the enemy can be put at a disadvantage at a critical time and place if we could covertly modify their picture of the weather, thereby influencing them to take detrimental courses of action. And, possibilities exist for intercepting enemy weather data bases and transmissions without their knowing.

2.0 INFORMATION OPERATIONS AND WARFARE

The force multipliers that are embodied within the Information War can be defined as see the enemy, hear and locate the enemy's command and control (C2) structure, disrupt the C2 structure by physical destruction, deny hostile C2 by jamming, and communicate and out think the enemy using a robust C2 system and assured seamless communications. These battlefield functions are supported by capabilities that include those listed in figure 1.



INFORMATION WAR FUNCTIONS

SEE
OWN THE NIGHT

KNOW THE ENEMY

HEAR
DISRUPT
DENY
OWN THE SPECTRUM
OFFENSIVE CONTROL

OWN THE SPECTRUM
DEFENSIVE CONTROL

COMMUNICATE &
OUTTHINK

DIGITIZATION
SITUATIONAWARENESS
COMMON PICTURE
HORIZONTAL INTEGRATION
OWN THE WEATHER
COMMUNICATIONS
sEAMLEss
ASSURED
SPLIT BASED

Figure 1. Information war functions.

Seamless Communications **– User transparent** communications from National Command Authority (NCA)to the individual soldier. Assured communications for split based operations and asset control from contractor to foxhole.

Own the Spectrum **–The most critical** resource required to win the information war is the electromagnetic spectrum. Sensors, information transport and smart weapons-smart munitions all require assured useof the spectrum. At the same time the enemy must be exploited and denied the use of the spectrum.

Digitized Battlefield - Common picture and situation awareness implemented horizontally across battlefield functional areas.

Own the Night - See and engage the enemy beyond his range day/night/all weather.

Own the Wedher - Operate smart weapons, smart munitions under ail weather conditions and provide the commander decision aids to plan/conduct all weather operations.

According to FM 100-6 Information Operations (1996), IO are military operations, supporting battle command, that enable, enhance and protect the commander's decision cycle and mission execution, while denying and exploiting the adversary's, to achieve an information advantage across the full range of operations. Information warfare (IW) is actions taken to preserve the integrity of one's INFOSYS from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary' INFOSYS and in the process achieving information dominance. Information dominance is that level of awareness where we know more about our battlespace and operations than an adversary.

3.0 WEATHER INFORMATION OPERATIONS

The objective of OTW IO is to guarantee and maximize our capability to anticipate and exploit the weather to our advantage while simultaneously denying the enemy the ability to use or manipulate the weather to their advantage. In general, this is accomplished by protecting our access to, integrity of, and use of our weather INFOSYS, and to exploit and attack the enemy's weather INFOSYS. There are three main components to weather information operations: weather intelligence, INFOSYS, and C2W. The remainder of this paper will focus on the military weather aspects of C2W. The thrust of OTW IO weather C2W has three parts, as summarized in figure 2.

WEATHER (WX) COMMAND AND CONTROL WARFARE (C2W) COMPONENTS	
WX C2W PROTECT	*Protect and secure our weather support INFOSYS (systems, databases, computers and communications, and personnel)
WX C2W EXPLOIT	*Understand enemy weather INFOSYS * Steal and utilize enemy weather data
WX C2W ATTACK	*Deny enemy weather information * Modify enemy weather data * Influence enemy weather picture

Figure 2. Weather Information Warfare

3.1 Weather C2W-Protect

With threats to our INFOSYS steadily increasing, priority of effort in the near term should be on implementing a C2W weather protect plan. Our ability to observe and know the weather conditions in the battlespace is of critical importance, since the rest of the weather supporting process hinges on this. Tactically, it is necessary to protect our capability to take forward weather observations, and to automate the relay of observations via secure Army systems. Key satellite controlled remote sensors must be camouflaged, and the use of tactical weather radar should be limited. Weather observing systems and communications can be especially vulnerable to enemy electronic jamming countermeasures. Weather data bases can also be easily corrupted.

At the strategic level, plans and procedures must be established to protect our weather INFOSYS and it's support structure. Some preventative actions include: a) identification of potential vulnerabilities in our weather INFOSYS and potential threat capabilities and intentions to attack our INFOSYS; b) use of secure communication paths, e.g., SIPRnet; c) defending meteorological satellite downlink sites, major communication paths/nodes and transmission sites, and centralized facilities and regional sites; and d) evaluating threat jamming capabilities and providing for alternate means when jammed.

3.2 Weather C2W-Exploit

In order to exploit the enemy one must first know and understand the enemy. Threat weather force structure and concept of operations can be deduced from their doctrine and exercises. Threat weather technology and capabilities can be determined through information gathered from the National Ground Intelligence Center and Air Intelligence Agency, and included in the commanders intelligence estimate and essential elements of information. With this information, key threat weather capabilities (e.g., weather radar) can be identified and targeted for exploitation.

"Weather" considerations should be included in overall intelligence exploitation procedures. Knowledge of the enemy's weather communications architecture can provide opportunities for interception of in clear and coded broadcasts. Other intelligence sources should be considered for the potential of extracting additional weather information. Finally, we must provide the means to relay threat weather data to friendly weather teams in a timely manner once it is acquired.

3.3 Weather C2W-Attack

A key aspect of IO and IW involves the trade-off between attacking and exploiting an opponent's INFOSYS, with respect to the need to affect information versus denying information. The most basic way of attacking information is to go after the communication channels. However, direct destruction of your enemy's communications channels also denies your access to these channels.

Similar to exploiting the enemy, in order to plan for attack one must fist know how the adversary uses weather information and what role it plays in their decision making process. It is also necessary to identify how the threat receives weather information and what type of information. C2W-attack weather involves not only physical destruction and denial, but also deceiving the enemy. The three main aspects of weather C2W-attack considered here are deny, influence, and change the weather.

3.3.1 Weather C2W-Attack: Deny

This involves denying the enemy the full picture of the battlespace weather situation by destroying their weather observing capability through physical destruction during a major regional conflict. Key threat weather observing sites such as weather radars, satellite ground stations, and satellite communications relay nodes should be included in the joint task force (JTF) target sets. Another means of denial is through disruption by electronic warfare. This can be accomplished by jamming threat weather system communication paths (e.g., high frequency transmissions of weather broadcasts in the area of operations) .

The enemy can also be denied weather information through the encryption of friendly sources. The encryption capabilities to use would be in mutual agreement with our allies. The Defense Meteorological Satellite Program (DMSP) provides secure data transmissions, and SIPRnet and the Joint Worldwide Intelligence Communication System (JWICS) classified systems should be used to carry routine weather data.

3.3.2 Weather C2W-Attack: Influence

The enemy can be deceived by hiding the real picture of the weather and in its place paint and insert a false weather picture. Weather deception considerations would be integrated into the major deception plans of the JTF commander and used only occasionally with key JTF deception actions. Options include transmitting false weather observations for enemy interception and the store/forward and transmission of modified weather satellite imagery with false timing (i.e., modified valid times).

For example, lets consider a role for meteorological satellites in potential deception plans. Prior to the deception action, threat forces would be allowed to directly receive in clear satellite transmissions. Then at a critical time, the threat's reception would be changed to acquire false imagery while friendly forces continue to receive the true imagery by encrypted link. Modification of the satellite image and/or header (i.e., valid date/time) could result in the delay of enemy planning of attack or defense strategy, throwing threat timing off enough for fast friendly strikes and delay of threat defensive actions. A scenario of altered imagery showing a weather front and heavy clouds moving into an area early could enable a movement of enemy forces expecting to be hidden from detection by the cloud cover to be caught out in the open.

3.3.3 Weather C2W-Attack: Change

It would be of great value to the Army to acquire even a modest capability to modify the weather, such as clearing fog or initiating precipitation over a selected but limited region. Currently, little progress is being made in this area, but in the future, improved knowledge and understanding of the physical processes affecting the weather may eventually provide a limited capability to modify weather effectively, if only locally. However, the military must follow International agreements not to modify weather in threat territory.

Some examples of the use of a limited capability to modify/clear adverse weather conditions include: a) fog dissipation at our -launch sites and landing zones when it would delay or stop operations; b) inducing precipitation over key areas to raise ceilings/visibility and enable launches; and c) eliminating ice fog in arctic artillery operations.

3.4 Summary of Weather C2W-Attack/Exploit Options and Objectives

3.4.1 Deny the Enemy

Leave the enemy with no weather picture or an incomplete picture through denial/disruption from electronic warfare or destruction of their weather INFOSYS. With no weather data, the enemy is denied information needed to take effective action and adjust his course of action.

3.4.2 Influence the Enemy

Trick the enemy with a skewed weather picture through deception and manipulation. Furthermore, once the deception is discovered by the enemy, he is left with an unreliable picture of the weather that he does not know if he can trust and will come to distrust his weather INFOSYS. With skewed weather information, the enemy can be influenced not to take action or to take the wrong action, or to take action at the wrong time and/or place.

3.4.3 Exploit the Enemy

Leave the enemy weather picture and INFOSYS undisturbed so we can steal and exploit their weather information, and so we can know what they know about the weather to help us predict expected enemy course of actions based on the weather. With in-tact, undisturbed weather information, the enemy can take their usual, expected actions based on the weather that we know about and can anticipate.

4.0 CONCLUSION

Weather IO guarantees and maximizes our ability to anticipate and exploit the weather to our advantage, and enables friendly forces to indeed "own the weather." The enemy must be denied access to meteorological satellite data in order to maximize our advantage and attain information dominance. Above all, we must protect our own weather INFOSYS and support capabilities. With threats to our INFOSYS increasing daily, the top priority of our weather c2w methodology is weather C2W-protect.

“Critical Army thrusts such as Digitize the Battlefield, Own the Night and Own the Weather are vital to winning the information war. . . Owning the Weather is one of the force multipliers that will ensure Land Force Dominance by giving the warfighter the information he needs to fight under all weather conditions. . . We will Own the Night and the Weather so we can support day, night, all weather operations.” -(General Jimmy D. Ross, 1994)